Claims

What is claimed is:

1. A method for detecting malicious code in an information handling system, comprising:

executing malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines;

applying the detection routines to executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of the detection routines; and

determining whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines.

2. The method of claim 1, wherein the detection routines include valid program detection routines and malicious code detection routines.

3. The method of claim 1, wherein the applying comprises:

applying the detection routines to gather information about the executable code under investigation by at least one of the following: examining the code or program; and searching for information in the information handling system about the code or program.

4. The method of claim 1, wherein determining whether the code under investigation is a valid program or malicious code includes scoring the execution of the detection routines as a function of the weights.

5. The method of claim 4, wherein scoring includes configuring a scoring algorithm to identify code under investigation as malicious code in response to at least one of a valid score and a malicious code score.

6. The method of claim 1, wherein the malicious code includes a trojan horse.

7. The method of claim 1, wherein the malicious code includes remote control software.

8. The method of claim 1, wherein the malicious code includes a keystroke logger.

9. The method of claim 1, wherein the malicious code includes spyware.

10. The method of claim 1, wherein the malicious code includes a worm.

11. The method of claim 1, wherein the malicious code includes a virus.

12. The method of claim 1, wherein the malicious code includes monitoring software.

13. A method for detecting malicious code in an information handling system, comprising:

executing malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines for gathering information about executable code under investigation, the detection routines including at least one of the following: (a) examining the code or program and (b) searching for information in the information handling system about the code or program, the detection routines including valid program detection routines and malicious code detection routines;

applying the detection routines to the executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of at least one of the detection routines; and

determining whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines, wherein determining whether the code under investigation is a valid program or malicious code includes scoring an execution of the detection routines as a function of the weights, and wherein scoring includes configuring a scoring algorithm to identify code under investigation as malicious code in response to at least one of a valid score and a malicious code score.

14. The method of claim 13, wherein the malicious code includes a trojan horse.

15. The method of claim 13, wherein the malicious code includes remote control software.

16. The method of claim 13, wherein the malicious code includes a keystroke logger.

17. The method of claim 13, wherein the malicious code includes spyware.

18. The method of claim 13, wherein the malicious code includes a worm.

19. The method of claim 13, wherein the malicious code includes a virus.

20. The method of claim 13, wherein the malicious code includes monitoring software.

21. A method for detecting malicious code on a information handling system, comprising:

executing detection routines, the detection routines examining at least one of the following: characteristics and behaviors of executable code under investigation;

assigning weights as a function of the examined characteristics and behaviors, the assigned weights indicative of a valid program or malicious code as a function of the detection routines; and

determining whether executable code under investigation is malicious code as a function of the weights assigned by the detection routines.

22. The method of claim 21, wherein the detection routines include valid program detection routines and malicious code detection routines.

23. The method of claim 21, wherein the valid program detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with a valid program; and

wherein the malicious code detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with malicious code.

24. The method of claim 21, wherein determining whether the executable code under investigation is malicious code includes scoring the execution of the detection routines as a function of the weights.

25. The method of claim 24, wherein scoring includes using a scoring algorithm for identifying executable code as malicious code in response to at least one of a valid score and a malicious code score.

26. The method of claim 25, wherein the scoring algorithm determines a valid program by a summation of weights of the valid program detection routines being greater than a valid program weight threshold, and a malicious code by a summation of weights of the malicious code detection routine having a summed value greater than a malicious code weight threshold.

27. The method of claim 26, wherein the scoring algorithm determines an anomalous program by the summation of weights of the valid program detection routines and the summation of weights of the malicious code detection routines both having sums greater than respective thresholds, or less than the respective thresholds.

28. The method of claim 21, and comprising:

operatively coupling the detection routines to an operating system of the information handling system via application programming interfaces (APIs).

29. The method of claim 21, wherein the detection routines access process behavior information of executable code under investigation.

30. The method of claim 21, wherein the characteristics and behaviors include at least one of the following: logging keystrokes, saving a display screen view, uploading files, downloading files, executing programs, and controlling the display screen.

31. The method of claim 21, wherein the detection routines access information about the executable code under investigation from an operating system of the information handling system via Application Programming Interfaces (APIs), and the detection routines gather information from executable code or a program by examining a binary image of the executable code or program, the characteristics and behavior of the executable code or program, and any other related code or programs used by the executable code under investigation.

32. The method of claim 21, and comprising:

delivering malicious code detection code (MCDC) containing the detection routines to the information handling system in a small compact code module via at least one of the following: a computer network, Internet, intranet, extranet, modem line, and prepackaged computer readable storage media.

33. The method of claim 21, wherein execution of the MCDC occurs in response to at least one of the following: a random initiation, an event driven initiation, and a periodic initiation.

34. The method of claim 21, wherein the malicious code includes a trojan horse.

35. The method of claim 21, wherein the malicious code includes remote control software.

36. The method of claim 21, wherein the malicious code includes a keystroke logger.

37. The method of claim 21, wherein the malicious code includes spyware.

38. The method of claim 21, wherein the malicious code includes a worm.

39. The method of claim 21, wherein the malicious code includes a virus.

40. The method of claim 21, wherein the malicious code includes monitoring software.

41. A computer program stored on computer-readable media for detecting malicious code in an information handling system, the computer program including instructions processable by the information handing system for causing the information handling system to:

execute malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines for gathering information about executable code under investigation, the detection routines including at least one of the following: (a) examining the executable code or program; and (b) searching for information in the information handling system about the executable code or program, the detection routines including at least one of valid program detection routines and malicious code detection routines;

apply the detection routines to the executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of at least one of the detection routines; and

determine whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines, wherein determining whether the code under investigation is a valid program or malicious code includes scoring an execution of the detection routines as a function of the weights, wherein scoring includes configuring a scoring algorithm to identify code under investigation as malicious code in response to at least one of a valid score and a malicious code score.

42. The computer program of claim 41, wherein the malicious code includes a trojan horse.

43. The computer program of claim 41, wherein the malicious code includes remote control software.

44. The computer program of claim 41, wherein the malicious code includes a keystroke logger.

45. The computer program of claim 41, wherein the malicious code includes spyware.

46. The computer program of claim 41, wherein the malicious code includes a worm.

47. The computer program of claim 41, wherein the malicious code includes a virus.

48. The computer program of claim 41, wherein the malicious code includes monitoring software.

49. A computer program stored on computer-readable media for detecting malicious code in an information handling system, the computer program including instructions processable by the information handling system for causing the information handling system to:

execute detection routines, the detection routines examining at least one of the following: characteristics and behaviors of executable code under investigation;

assign weights as a function of the examined characteristics and behaviors, the assigned weights indicative of a valid program or malicious code as a function of the detection routines; and

determine whether executable code under investigation is malicious code as a function of the assigned weights.

50. The computer program of claim 49, wherein the detection routines include valid program detection routines and malicious code detection routines.

51. The computer program of claim 49, wherein the valid program detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with a valid program; and

wherein the malicious code detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with malicious code.

52. The computer program of claim 49, wherein determining whether the executable code under investigation is malicious code includes scoring the execution of the detection routines as a function of the weights.

53. The computer program of claim 52, wherein scoring includes using a scoring algorithm for identifying executable code as malicious code in response to at least one of a valid score and a malicious code score.

54. The computer program of claim 53, wherein the scoring algorithm determines a valid program by a summation of weights of the valid program detection routines being greater than a valid program weight threshold, and a malicious code by a summation of weights of the malicious code detection routine having a summed value greater than a malicious code weight threshold.

55. The computer program of claim 54, wherein the scoring algorithm determines an anomalous executable code under investigation by the summation of weights of the valid program detection routines and the summation of weights of the malicious code detection routines both having sums greater than respective thresholds, or less than the respective thresholds.

56. The computer program of claim 49, and comprising instructions processable by the information handling system for causing the information handling system to:

operatively couple the detection routines to an operating system of the information handling system via application programming interfaces (APIs).

57. The computer program of claim 49, wherein the detection routines access process behavior information of executable code under investigation.

58. The computer program of claim 49, wherein the characteristics and behaviors include at least one of the following: logging keystrokes, saving a display screen view, uploading files, downloading files, executing programs, and controlling the display screen.

59. The computer program of claim 49, wherein the detection routines access information about the executable code under investigation from an operating system of the information handling system via Application Programming Interfaces (APIs), and the detection routines gather information from executable code or a program by examining a binary image of the executable code or program, the characteristics and behavior of the executable code or program, and any other related code or programs used by the executable code under investigation.

60. The computer program of claim 49, comprising instructions processable by the information handling system for causing the information handling system to:

deliver malicious code detection code (MCDC) containing detection routines to the information handling system in a small compact code module via at least one of the following: a computer network, Internet, intranet, extranet, modem line, and prepackaged computer readable storage media.

61. The computer program of claim 49, wherein execution of the MCDC occurs in response to at least one of the following: a random initiation, an event driven initiation, and a periodic initiation.

62. The computer program of claim 49, wherein the malicious code includes a trojan horse.

63. The computer program of claim 49, wherein the malicious code includes remote control software.

64. The computer program of claim 49, wherein the malicious code includes a keystroke logger.

65. The computer program of claim 49, wherein the malicious code includes spyware.

66. The computer program of claim 49, wherein the malicious code includes a worm.

67. The computer program of claim 49, wherein the malicious code includes a virus.

68. The computer program of claim 49, wherein the malicious code includes monitoring software.

69. An information handling system, comprising:

a memory;

a processor; and

computer-readable code stored by the memory and processable by the processor for detecting malicious code, the computer-readable code including instructions for causing the processor to:

execute malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines for gathering information about executable code under investigation, the detection routines including at least one of the following: (a) examining the executable code or program and (b) searching for information about the executable code or program in the information handling system, the detection routines including valid program detection routines and malicious code detection routines;

apply the detection routines to the executable code under investigation, the detection routines assigning weights to respective executable code under investigation in response to detections of a valid program or malicious code as a function of at least one of the detection routines; and

determine whether executable code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines, wherein determining whether the code under investigation is a valid program or malicious code includes scoring an execution of the detection routines as a function of the weights, and wherein scoring includes configuring a scoring algorithm to identify executable code under investigation as malicious code in response to at least one of a valid score and a malicious code score.

70. The information handling system of claim 69, wherein the malicious code includes a trojan horse.

71. The information handling system of claim 69, wherein the malicious code includes remote control software.

72. The information handling system of claim 69, wherein the malicious code includes a keystroke logger.

73. The information handling system of claim 69, wherein the malicious code includes spyware.

74. The information handling system of claim 69, wherein the malicious code includes a worm.

75. The information handling system of claim 69, wherein the malicious code includes a virus.

76. The information handling system of claim 69, wherein the malicious code includes monitoring software.

77. An information handling system, comprising:

a memory;

a processor; and

computer-readable code stored by the memory and processable by the processor for detecting malicious code on the information handling system, the computer-readable code including instructions for causing the processor to:

execute detection routines, the detection routines examining at least one of the following: characteristics and behaviors of programs;

assign weights as a function of the examined characteristics and behaviors, the assigned weights indicative of a valid program or malicious code as a function of the detection routines; and

determine whether executable code under investigation is malicious code as a function of the weights assigned by the detection routines.

78. The information handling system of claim 77, wherein the detection routines include valid program detection routines and malicious code detection routines.

79. The information handling system of claim 77, wherein the valid program detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with a valid program; and

wherein the malicious code detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with malicious code.

80. The information handling system of claim 77, wherein determining whether the executable code under investigation is malicious code includes scoring the execution of the detection routines as a function of the weights.

81. The information handling system of claim 80, wherein scoring includes using a scoring algorithm for identifying executable code as malicious code in response to a valid score and a malicious code score.

82. The information handling system of claim 81, wherein the scoring algorithm determines a valid program by a summation of weights of the valid program detection routines being greater than a valid program weight threshold, and a malicious code by a summation of weights of the malicious code detection routine having a summed value greater than a malicious code weight threshold.

83. The information handling system of claim 82, wherein the scoring algorithm determines an anomalous executable code under investigation by the summation of weights of the valid program detection routines and the summation of weights of the malicious code detection routines both having sums greater than respective thresholds, or less than the respective thresholds.

84. The information handling system of claim 77, wherein the characteristics and behaviors include at least one of the following: logging keystrokes, saving a display screen view, uploading files, downloading files, executing programs, and controlling the display screen.

85. The information handling system of claim 77, wherein the detection routines access information about the executable code under investigation from an operating system of the information handling system via Application Programming Interfaces (APIs), and the detection routines gather information from executable code or a program by examining a binary image of the executable code or program, the characteristics and behavior of the executable code or program, and any other related code or programs used by the executable code under investigation.

86. The information handling system of claim 77, wherein the computer-readable code includes instructions for delivering the MCDC containing detection routines to the information handling system in a small compact code module via at least one of the following: a computer network, Internet, intranet, extranet, modem line, and prepackaged computer readable storage media.

87. The information handling system of claim 77, wherein execution of the MCDC occurs in response to at least one of the following: a random initiation, an event driven initiation, and a periodic initiation.

88. The information handling system of claim 77, wherein the malicious code includes a trojan horse.

89. The information handling system of claim 77, wherein the malicious code includes remote control software.

90. The information handling system of claim 77, wherein the malicious code includes a keystroke logger.

91. The information handling system of claim 77, wherein the malicious code includes spyware.

92. The information handling system of claim 77, wherein the malicious code includes a worm.

93. The information handling system of claim 77, wherein the malicious code includes a virus.

94. The information handling system of claim 77, wherein the malicious code includes monitoring software.

95. A method for detecting malicious code in an information handling system, comprising:

executing malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines;

applying the detection routines to code under investigation, the detection routines associating weights to respective code under investigation in response to detections of malicious code as a function of the detection routines; and

determining whether code under investigation is malicious code as a function of the weights associated by the detection routines.

96. The method of claim 95, wherein the applying comprises:

applying the detection routines to gather information about the code under investigation by at least one of the following: examining the code under investigation; and searching for information in the information handling system about the code under investigation.

97. The method of claim 95, wherein determining whether the code under investigation is malicious code includes scoring the execution of the detection routines as a function of the weights, wherein scoring includes configuring a scoring algorithm to identify the code under investigation as malicious code in response to a malicious code score.

98. The method of claim 95, wherein the malicious code includes a trojan horse.

99. The method of claim 95, wherein the malicious code includes remote control software.

100. The method of claim 95, wherein the malicious code includes a keystroke logger.

101. The method of claim 95, wherein the malicious code includes spyware.

102. The method of claim 95, wherein the malicious code includes a worm.

103. The method of claim 95, wherein the malicious code includes a virus.

104. The method of claim 95, wherein the malicious code includes monitoring software.